REMARKS

Claims 1-36 are currently pending in the patent application. The Examiner has objected to the drawings, has rejected Claims 10-27 under 35 USC 112 as indefinite; and, has rejected Claims 1-36 under 35 USC 103 as unpatentable over Coley in view of Belissent.

In response to the rejection of the drawings, Applicants submit herewith an "Annotated Sheet" including Fig. 2 with text included in the boxes. A formal version of the annotated drawing will be submitted once the changes have been approved by the Examiner.

The Examiner has rejected all of the claims as being unpatentable over the combined teachings of Coley and Belissent. Applicants respectfully assert that the invention, as set forth in the amended claims, is patentably distinct from the cited references.

The present application teaches and claims apparatus, a method, a processor, and a program storage device for data processing wherein bit streams of data exchanged between a network resource server and a data network are passed through a network processor. The network processor monitors the data flow rate of data passing through it to and from any data sources. A first derivative of the data flow rate

is computed to determine the rate of change of the data flow rate and actions are taken based upon the rate of change of the data flow rate. Actions taken include selectively discarding data flowing toward the network resource server (Claims 28-35), or modifying instructions loaded into the instruction memory in response to the determined rate of change (Claims 1-27 and 36).

The invention is able to detect a denial of service (DoS) attack based on the change in the data flow rate into or out of the server (note, for example, that Claim 19 recites monitoring data flow outbound from the server). Further, the invention is able to detect a DoS attack even if the attack is being mounted from multiple different IP addresses. Accordingly, the present invention does not look simply at requests for connection from single client IP addresses; but, looks at the overall data flow rate to the server from any data source and from the server to any locations.

Applicants respectfully assert that the invention as claimed is not rendered obvious by the cited references. The Coley patent is directed to a firewall system for protecting network elements connected to a public network. The firewall (210 of Fig. 2) is disposed between the network (202) and the network elements (216 and 218) to be

protected. Additionally disposed between the firewall and the computer network is a so-called "publicly accessible system" including a web server, port and e-mail. The Examiner contends that the firewall 210 is analogous to the claimed network processor coupled to a network server (see: the top of page 4 of the Office Action). The Examiner cites the illustrated firewall 210 and the teachings found in Col. 7 against the claimed network processor comprising a plurality of interface processors, instruction memory, data memory and a plurality of input/output (hereinafter "I/O") ports. However, the Coley patent clearly teaches in Col. 7 that the firewall is an application. Coley does not teach or suggest that its firewall 210 has a plurality of processors, instruction memory and data memory and a plurality of I/O ports.

Further, the Examiner states that the one of the I/O ports is for exchanging data passing through the network processor, citing 206 as the network processor, with an external network. The Examiner has, therefore, cited two different components of the Coley system, firewall 210 and the "publicly accessible system" 206 (including the web server and e-mail system), against the network processor of the claims. Moreover, the Coley component 206 with its "internal network port" is not part of the firewall system

and does not operate under the direction of interface processors which are part of a firewall, since Coley does not teach or suggest that the firewall comprises interface processors.

Applicants further assert that the Coley patent does not teach or suggest the claimed feature of monitoring data flow addressed to the network server and modifying instructions based on the data flow, as the Examiner concludes at the bottom of page 4 and top of page 5 of the Office Action. What the cited teachings of Coley describe, at Col. 6, lines 5-20, is that the firewall application provides proxies to verify incoming access requests to ascertain if the requester is authorized to access the network components behind the firewall. Coley does not teach or suggest that the incoming data rate be monitored nor does Coley teach or suggest taking actions based on a data flow rate of change derived from the data flow rate. Packet filtering as taught by Coley in Col. 6, at lines 48-50 does not teach or suggest modifying instructions. Moreover, the cited line 65 from Col. 7, simply mentions a set of verification tests, which does not teach or suggests a step or means to modify instructions.

The Examiner has acknowledged, at the top of page 5, that the Coley patent does not teach or suggest monitoring

the rate of data flow addressed to a network resource server, deriving data flow rate over time to determine the rate of change of data flow, and modifying instructions based on the derived data flow rate over time. The Examiner has cited the Belissent patent which teaches a method for thresholding and throttling client connection requests to prevent denial of service (DoS) attacks. Applicants reiterate the argument that one having ordinary skill in the art would not look to modify the Coley patent with the teachings of the Belissent patent. Since Coley provides a firewall to prevent unauthorized users from obtaining access to the network components located behind the firewall, no attacker would have access to the network components to flood the components with requests in such a way as to cause a DoS situation. Denial of Service (DoS) attacks are directed against publicly accessible components, and operate by flooding the publicly accessible components (e.g., the web server of 206 in Coley) with requests to overwhelm the server. Since Coley does not allow unauthorized requests to get past the firewall, there would be no way for a DoS attacker to get the requests past the firewall. Accordingly, there would be no reason for Coley to modify its firewall to include a component which determines a

connection request rate in accordance with the teachings of Belissent.

Moreover, Applicants believe that even if one were to modify Coley with Belissent, one would not arrive at the invention as claimed. The Belissent patent describes, in the cited teachings from Col. 4, lines 10-25, that the IP throttler records all connecting IP addresses and the number of connections per client address is recorded. "If a particular client's connection request rate is greater than a rejection threshold associated with that client, the IP throttler will refuse any new connections from the client until the beginning of the next throttling period". Belissent simply looks at the number of connection requests from each client address. If a DoS attack is mounted from multiple locations, with multiple requests for connection from different client addresses, the Belissent system will not detect the DoS attack. Moreover, Belissent cannot detect a DoS attack based on server activity (i.e., the data flow rate outbound from the server) which may be the result of a single client request based on a single client request for connection. The amended claim language expressly recites that the present invention monitors the rate of data flow addressed to the network server from any data source (Claims 1-9, 10-18 and 36), monitors the rate of data flow

outbound from the server (Claims 19-27), and monitors the rate of data flow in and out of the server (Claims 28-35). Applicants respectfully assert that the combined teachings of Coley and Belissent do not teach or suggest the claimed monitoring.

Applicants further assert that neither Belissent nor Coley teaches computing the derivative of a monitored data flow rate to determine a rate of change of data flow, and neither teaches taking action based on a determined rate of change of data flow. Accordingly, it cannot be concluded that a Coley system having a Belissent connection request flow thresholding component would obviate the invention as claimed. If one were to modify Coley to include a component for determining a connection request rate at its firewall, one would still not have means or steps for monitoring the rate of data flow addressed to the network resource server from all data sources, means or steps for monitoring the rate of data flow outbound from the server, means or steps for monitoring the rate of data flow in and out of the server, at least one interface processor component computing a derivative of data flow rate over to time determine the rate of change of data flow and for either modifying instructions or discarding data based on the determined rate of change of data flow. Accordingly, Applicants conclude

that the Examiner has not established a *prima facie* case of obviousness.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

C. S. Lingafelt, et al

By: Anne Vachon Dougherty

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910

ANNOTATED SHEET

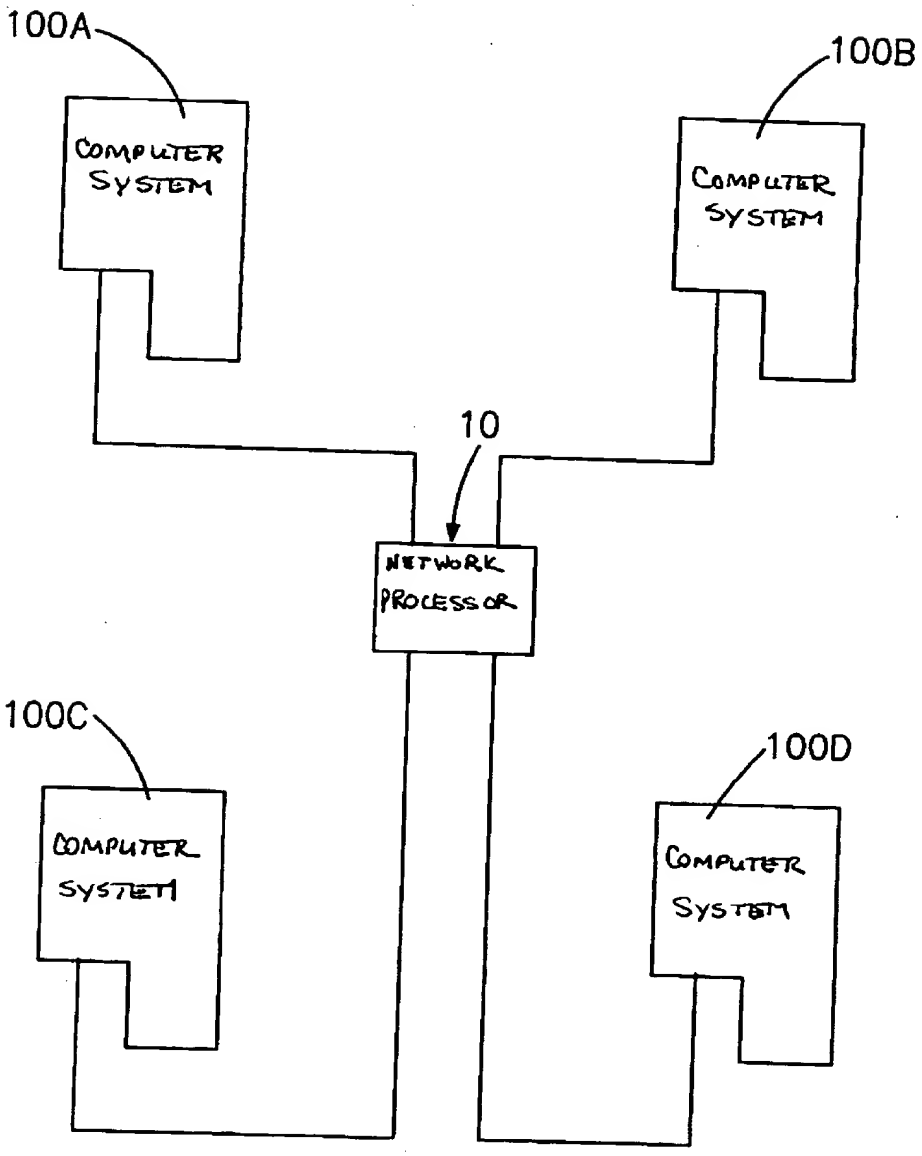

FIG. 2